

Y_tohamy@hotmail.com

www.elnems.8k.com

جمهورية مصر العربية – الجيزة

طالب بالمعهد العالي للدراسات المتطورة بالهرم ٢٠٠٤ – ٢٠٠٨

- **كتاب مجاني لكل مسلم ومسلمة.**
- **كتاب تعليمي يعلمك ما هو تفكير الهاكر "المخترق" حتى تأخذ منه الحذر.**
- **للمبتدأين و المحترفين أيضا.**

بسم الله الرحمن الرحيم

"سبحانك لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم"

صدق الله العظيم

سلسلة فنون وخدع الهاكرز

جمع وتأليف: ياسر رجب التهامي – ٣٠سنة (١٩٨٤)

هذا الكتاب تعليمي للحماية من الهاكر وأساليبهم وقد تم تجميع بعض المعلومات من الشبكة و الكاتب غير مسئول عن أية نتائج تصدر من استخدام الكتاب استخداماً خاطئاً.

مقدمة

السلام عليكم ورحمة من الله تعالى وبركاته

أما بعد،.......... قد أعددت هذا الكتاب لكل مبتدىء ومبتدئة ومرجع للمحترف والمحترفة ولتعليم حيل الهاكر للحماية منهم بجميع الوسائل وأرجو ان ينال إعجابكم ان شاء الله

☺

وقد قَسّمت هذه السلسة إلى الآتي:

نبدأ

تعريف الهكرز

تاريخ الهكرز.

ما هو الآي بي IP.

التعرف إذا تم اختراق جهازك أم لا.

الحلول لتنظيف جهازك إذا تم اختراقه.

تفصيل عن اختراق الأجهزة.

تفصيل عن اختراق المواقع.

شرح بعض برامج الهاكرز الهامة والفعالة.

بعض النصائح لحماية جهازك من القرصنة (الهاكرز)

١٥ نصيحة لتكون هاكر محترف.

بعض المواقف مع الهكرز .... ومنها ما تم معي ☺

نبذة عن الفيروسات

انتهى

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

بسم الله والصلاة والسلام على رسول الله الكريم و على من والاه إلى يوم الدين

أما بعد .... يا أخي........ يا أختي........ أستحلفكم بالله العظيم ان لا تستخدموا الاختراق في ضرر المسلمين أو أي شخص بريء حتى وان كان نصرانياً أو يهودياً إلا بالحق و بذلك قد أكون قد خلصت ذمتي ☹.

والآن نبدأ بعون الله أول درسنا:

الدرس الأول

(نبذة سريعة وشاملة عن الهاكرز)

قد جعلت الدرس الأول شامل لجميع حيل الهاكر من بداية تعريفه وكيف يتم وكيف تحمي الجهاز ...... الخ. ثم بعد هذا الدرس سأبدأ بشرح كل جزءٍ على حدا.

نبدأ بسم الله

تعريف الهكرز:

- تسمى باللغة الإنجليزية (Hacking).. وتسمى باللغة العربية عملية التجسس أو الاختراق أو القرصنة .. حيث يقوم أحد الأشخاص الغير مصرح لهم بالدخول إلى نظام التشغيل في جهازك بطريقة غير شرعية ولأغراض غير سوية مثل التجسس أو السرقة أو التخريب حيث يتاح للشخص المتجسس (الهاكر) ان ينقل أو يمسح أو يضيف ملفات أو برامج كما انه بمكانه ان يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو التخزين .. ولكن بالطبع هذا لا يتماشى مع أخلاق المسلم فلذلك سنتعلم كل ما يفعله الهاكرز لكي نكون حريصين منهم.

و أيضا الاختراق بصفه عامه هو قدرة الفرد من خلال الانترنت الوصول أو عمل بعض العمليات بطريقة غير شرعية سواء حصل على معلومات أو دخل احد الأجهزة أو المواقع... و ذلك بالتحايل على الأنظمة و الدخول فيها..

أولا يجب ان نتعرف على المخترق ... من هو الهاكر ؟

هو الشخص الذي يستمتع بتعلم لغات البرمجة و أنظمة التشغيل الجديدة.

هو الشخص الذي يستمتع بعمل البرامج أكثر من تشغيل هذه البرامج و أيضا يحب ان يتعلم المزيد عن هذه البرامج.

هو الشخص الذي يؤمن بوجود أشخاص آخرين يستطيعون القرصنة.

هو الشخص الذي يستطيع ان يصمم و يحلل البرامج أو انظمه التشغيل بسرعة.

هو شخص خبير بلغة برمجة ما أو نظام تشغيل معين ..

تاريخ الهاكرز :

======

قبل عام ١٩٦٩:

في هذه السنوات لم يكن للكمبيوتر وجود و لكن كان هناك شركات الهاتف و التي كانت المكان الأول لظهور ما نسميهم بالهاكرز في وقتنا الحالي. و لكي نلقي بالضوء على طريقة عمل الهاكرز في تلك الفترة الزمنية نعود للعام ١٨٧٨ في الولايات المتحدة الأمريكية و في إحدى شركات الهاتف المحلية.. كان أغلب العاملين في تلك الفترة من الشباب المتحمس لمعرفة المزيد عن هذه التقنية الجديدة و التي حولت مجرى التاريخ.

فكان هؤلاء الشباب يستمعون إلى المكالمات التي تجرى في هذه المؤسسة و كانوا يغيروا من الخطوط الهاتفية فتجد مثلا هذه المكالمة الموجهة للسيد مارك تصل للسيد جون.. و كل هذا كان بغرض التسلية و لتعلم المزيد .. و لهذا قامت الشركة بتغيير الكوادر العاملة بها إلى كوادر نسائية.

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

في الستينات من هذا القرن ظهر الكمبيوتر الأول. لكن هؤلاء الهاكرز كانوا لا يستطيعون الوصول لهذه الكمبيوترات و ذلك لأسباب منها كبر حجم هذه الآلات في ذلك الوقت و وجود حراسة على هذه الأجهزة نظرا لأهميتها ووجودها في غرف ذات درجات حرارة ثابتة .

و لكن متى ظهرت تسمية هاكرز ؟ الغريب في الأمر ان في الستينات الهاكر هو مبرمج بطل أو عبقري .. فالهاكرز في تلك الفترة هو المبرمج الذي يقوم بتصميم أسرع برنامج من نوعه و يعتبر دينيس ريتشي و كين تومسون أشهر هاكرز على الإطلاق لأنهم صمموا برنامج إلى ونكس و كان يعتبر الأسرع و ذلك في عام ١٩٦٩.

العصر الذهبي للهاكرز - ١٩٨٠ - ١٩٨٩

في عام ١٩٨١ أنتجت شركة IBM المشهورة جهاز أسمته بالكمبيوتر الشخصي يتميز بصغر حجمه و سهولة استخدامه و استخدامه في أي مكان و أي وقت .. و لهذا فقد بدأ الهاكرز في تلك الفترة بالعمل الحقيقي لمعرفة طريقة عمل هذه الأجهزة و كيفية تخريب الأجهزة .

و في هذه الفترة ظهرت مجموعات من الهاكرز كانت تقوم بعمليات التخريب في أجهزة المؤسسات التجارية .

في عام ١٩٨٣ ظهر فيلم سينمائي اسمه (حرب الألعاب) تحدث هذا الفيلم عن عمل الهاكرز و كيف ان الهاكرز يشكلون خطورة على الدولة و على اقتصاد الدولة و حذر الفيلم من الهاكرز .

حرب الهاكرز العظمى - ١٩٩٠ - ١٩٩٤

البدايات الأولى لحرب الهاكرز هذه في عام ١٩٨٤ حيث ظهر شخص اسمه (ليكس لوثر) و انشأ مجموعة أسماها (LOD) و هي عبارة عن مجموعة من الهاكرز الهواة و الذي يقومون بالقرصنة على أجهزة الآخرين. وكانوا يعتبرون من أذكى الهاكرز في تلك الفترة. إلى ان ظهرت مجموعة أخرى اسمها (MOD) و كانت بقيادة شخص يدعى (فيبر). و كانت هذه المجموعة منافسة لمجموعة (LOD) . و مع بداية العام ١٩٩٠ بدأت المجموعتان بحرب كبيرة سميت بحرب الهاكرز العظمى و هذه الحرب كانت عبارة عن محاولات كل طرف اختراق أجهزة الطرف الآخر . و استمرت هذه الحرب ما يقارب الأربعة أعوام و انتهت بإلقاء القبض على (فيبر) رئيس مجموعة (MOD) و مع انتهاء هذه الحرب ظهر الكثير من المجموعات و من الهاكرز الكبار

تاريخ الهاكرز في الولايات المتحدة:

قبل البدء في الحديث عن الهاكرز في الولايات المتحدة و قصة قرصنة جريدة نيويورك تايمز . نتحدث عن (كيفن ميتنيك) أشهر هاكر في التاريخ .
كيفن متينيك قام بسرقات كبيرة دوخت الإف بي آي و لم يستطيعوا معرفة الهاكر في أغلب سرقاته .. في مرة من المرات استطاع ان يخترق شبكة الكمبيوترات الخاصة بشركة Digital Equipment Company و تم القبض علية في هذه المرة و سجنه لمدة عام . و بعد خروجه من السجن كان أكثر ذكاء . فكانوا لا يستطيعون ملاحقته فقد كان كثير التغيير من شخصيته كثير المراوغة في الشبكة .. من أشهر جرائمه سرقة الأرقام الخاصة ب ٢٠٠٠٠ بطاقة ائتمان . و التي كانت آخر جريمة له تم القبض بعدها علية و سجنه لمدة عام . ولكن إلى الآن لم يخرج من السجن لان الإف بي آي يرون بان كيفن هذا خطير و لا توجد شبكة لا يستطيع اختراقها ظهرت أصوات تطالب الحكومة بالإفراج عن كيفن و ظهرت جماعات تقوم بعمليات قرصنة باسم كيفن من بينها قرصنة موقع جريدة نيويورك تايمز و التي ظهرت شاشتها متغيرة كثيرا في مرة من المرات و ظهرت كلمات غريبة تعلن للجميع بان هذه الصفحة تم اختراقها من قبل كيفن ميتنيك . ولكن تبين بعد ذلك بأنه أحد الهاكرز الهواة المناصرين لميتنيك.

معنى و أنواع الكراكرز:

قد لا يستصيغ البعض كلمة كراكرز التي أدعو بها المخربين هنا لأنه تعود على كلمة هاكرز ولكني سأستخدمها لأعني به المخربين لأنظمة الكمبيوتر وهم على كل حال ينقسمون إلى قسمين :

١- المحترفون: هم إما ان يكونوا ممن يحملون درجات جامعية عليا تخصص كمبيوتر ومعلوماتية ويعملون محللي نظم ومبرمجين ويكونوا على دراية ببرامج التشغيل ومعرفة عميقة بخباياها والثغرات الموجودة بها. تنتشر هذه الفئة غالبا بأمريكا وأوروبا ولكن انتشارهم بداء يظهر بالمنطقة العربية (لا يعني هذا ان كل من يحمل شهادة عليا بالبرمجة هو بأي حال من الأحوال كراكر) ولكنه متى ما أقتحم الأنظمة عنوة مستخدما أسلحته البرمجية العلمية في ذلك فهو بطبيعة الحال احد المحترفين.

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

٢- الهواة: إما ان يكون احدهم حاملا لدرجة علمية تساندة في الإطلاع على كتب بلغات أخرى غير لغته كالأدب الإنجليزي أو لديه هواية قوية في تعلم البرمجة ونظم التشغيل فيظل مستخدما للبرامج والتطبيقات الجاهزة ولكنه يطورها حسبما تقتضيه حاجته ولربما يتمكن من كسر شفرتها البرمجية ليتم نسخها وتوزيعها بالمجان. هذا الصنف ظهر كثيرا في العامين الآخرين على مستوى المعمورة وساهم في انتشاره عاملين . الأول: انتشار البرامج المساعدة وكثرتها وسهولة التعامل معها . والأمر الثاني: ارتفاع أسعار برامج وتطبيقات الكمبيوتر الأصلية التي تنتجها الشركات مما حفز الهواة على إيجاد سبل أخرى لشراء البرامج الأصلية بأسعار تقل كثيرا عما وضع ثمنا لها من قبل الشركات المنتجة.

ينقسم الهواة كذلك إلى قسمين :

١- الخبير: وهو شخص يدخل للأجهزة دون إلحاق الضرر بها ولكنه يميل إلى السيطرة على الجهاز فتجده يحرك المأوس عن بعد أو يفتح مشغل الأقراص بقصد السيطرة لا أكثر .

٢- المبتدئ: هذا النوع أخطر الكراكرز جميعهم لأنه يحب ان يجرب برامج الهجوم دون ان يفقه تطبيقها فيستخدمها بعشوائية لذلك فهو يقوم أحيانا بدمار واسع دون ان يدري بما يفعله.

الكراكرز بالدول العربية:

للأسف الشديد كثير من الناس بالدول العربية يرون بان الكراكرز هم أبطال بالرغم ان العالم كله قد غير نظرته لهم. فمنذ دخول خدمة الانترنت للدول العربية في العام ١٩٩٦ تقريبا والناس يبحثون عن طرق قرصنه جديدة وقد ذكرت آخر الإحصائيات بان هناك أكثر من ٨٠% من المستخدمين العرب تحتوي أجهزتهم على ملفات باتش وهي ملفات تسهل عمل الكراكرز .

الكراكرز بدول الخليج العربي :

انتشرت ثقافة الكراكرز كثيرا بدول الخليج العربي خصوصا بالسعودية على رغم دخولها المتأخر لخدمة الانترنت (يناير ١٩٩٩) حيث كثرت الشكاوى من عدة أفراد وشركات وقد بين الاستبيان الذي أجرته مجلتين عربيتين متخصصتين هما بي سي و انترنت العالم العربي ان بعض الأجهزة بالدول الخليجية تتعرض لمحاولات اختراق مرة واحدة على الأقل يوميا.

كيف يتم الاختراق :

==========

للاختراق طرق عديدة فكل هاكر يكون لنفسه أساليب خاصة به لكن في النهاية يستخدم الجميع نفس الأسس التي تمكن الهاكر من الوصول إلى مبتغاة ..

اختراق الأجهزة

بعض القواعد الأساسية لاختراق جهاز معين:

=========================

يتم اختراق جهاز معين عن طريق منفذ مفتوح (Open Port) في جهاز الضحية و الذي يسمح للمخترق للدخول في الجهاز و التحكم فيه و هذا النوع من الاختراق يسمى (Client/Server) وهو عن طريق إرسال ملف الباتش (Patch) والذي يفتح منفذ في جهاز الضحية و الذي يتسلل منه المخترق إلى جهاز الضحية عن طريق البرنامج نفسه كما ان الهكرز المحترفين عندما يعرفون الآي بي الخاص بالضحية يفعلون ما يسمى بسكان على الآي بي و من ثم يستخدمون البرنامج المناسب للمنفذ أو يقومون بعمل برامج خاصة بهم للنفاذ من منفذ معين، كما انه يمكن للمخترق أيضا ان يخترق عن طريق النت بيوس (Net Bios) أو عن طريق الدوس (Dos) و العديد من الطرق الأخرى، و نستطيع ان نقول ان أكثر الهكرز احترافا هم المتسللين عن طريق ثغرات النظام وهذه النقطة سندرسها بتوسع ان شاء الله ..

الاتصال بشبكة الانترنت:

=============

لا يستطيع الهاكر ان يدخل إلى جهازك إلا إذا كنت متصلاً بشبكة الانترنت أما إذا كان جهازك غير متصل بشبكة الانترنت أو أي شبكة أخرى فمن المستحيل ان يدخل أحد إلى جهازك سواك، ولذلك إذا أحسست

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

بوجود هاكر في جهازك فسارع إلى قطع الاتصال بخط الانترنت بسرعة حتى تمنع الهاكر من مواصلة العبث والتلصص في جهازك ..

برنامج التجسس:

=========

حتى يتمكن الهاكر العادي من اختراق جهازك لابد ان يتوافر معه برنامج يساعده على الاختراق !
ومن أشهر برامج الهاكرز هذه البرامج :
Web Cracker 4
Net Buster
NetBus Haxporg
Net Bus 1.7
Girl Friend
BusScong
BO Client and Server
Hackers Utility

ولكن الآن كل هذه البرامج لا تعمل دون جدوى وذلك لان ملف الباتش الخاص بها يمسك من قبل برامج الحماية العادية مثل النورتن والمكافي وغيرها.
و أما البرامج الحديثة التي نزلت ولا ترى من قبل برامج الحماية من الفيروسات هي :
١- BEAST
٢- CIA122b
٣- OptixPro
٤- NOVA
٥- غيرها من البرامج الشهيرة.
٦- وبالتأكيد طبعا البرامج التي صممتها بنفسك على لغة برمجة معينة فبالتالي يمكنك ان تضيف عليها أشياء لا ترى من قبل برامج الحماية.

ولكن الآن وحديثا كل ما نزل برنامج ما من برامج الاختراق فانه يتم عمل حماية له من قبل برامج الحماية، لذلك يفضل ان يكون لك برنامج اختراق خاص بك ويكون مختلف تماما عن أي برنامج آخر من برامج التروجان لكي لا يتم كشفه من برامج الحماية.

اختراق الأجهزة:

=======

و يكون نوعين : -
١- **هاك بالثغرات** : موضوع طويل و معقد نوعا ما و صعب و يستخدمه الخبراء و المحترفين.

٢- **هاك بالبتشات**: سهل و بسيط و سريع و قوي نوعا ما و عاده ما نبدء به.

أولا : الهاك بالبتشات (السيرفر) أحصنة طروادة

الـ Server معناه بالعربي خادم أو كما يطلق عليه باتش أو أحصنة طروادة أو تروجان وهو عبارة عن ملف دائما ما يذهب للضحية حتى يتم اتصال بينه وبين الملف الرئيسي ومن خلاله تستطيع التحكم بالجهاز تحكما كاملا على حسب البرنامج الذي تستخدمه في الاختراق، كما ان اي برنامج باتشات في عالم الحاسبات تم برمجته على ٤ أشياء أساسية وهم:
١- *ملف الباتش* server: وهو ملف يجب إرساله للضحية و يجب على الضحية فتحه أيضا حتى يفتح عنده منفذ (port) ثم نستطيع اختراقه ..
٢- *ملف* Edit server : وهو لوضع إعدادات الباتش أو تغييرها.
٣- *ملف البرنامج الأساسي* Client: وهو الذي تتصل به للضحية و تتحكم في جهازه ..
٤- ملفات الـ dll و غيرها وهي التي تساعد البرنامج على التشغيل ومن دونها لا يعمل البرنامج ..
كما ان أي باتش دائما ما يكون امتداده بـ name.exe حيث Name تعني اسم السيرفر و exe. تعني امتداده، والامتداد عبارة عن شيء خاص لتشغيل الملف فمثلا دائما ما يكون امتداد الصور بهذه الامتدادات (JPG – BMP – GIF .... الخ) ويكون امتداد ملفات الورد (DOC) وملفات الأكسل (XLS) وملفات الأغاني (MP3 – WAV ...)و امتداد ملفات الفيديو (........ - AVI – ASF – MPG).
لذلك فان امتداد البرامج الأساسية أو ما يطلق عليها البرامج التنفيذية بالطبع دائما ما يكون امتدادها (EXE) لذلك يجب عند إرسال ملف الباتش عدم إرساله كما هو exe. بل يجب إخفائه للتحايل في إرساله حيث

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

يمكنك إرساله مدمج مع صوره أو ملف تنصيب عن طريق بعض البرامج، و من الممكن تغير امتداد الباتش عن طريق الدوس حتى لا يشك الضحية .. وسنذكر الطريقة ان شاء الله.

الكي لوجر Key Logger

الكي لوجر هو برنامج صغير يتم تشغيله داخل جهاز الحاسب ودائما ما يكون مع ملف السيرفر "حصان طروادة" لكي يقوم بأغراض التجسس على أعمالك التي تقوم بها على حاسبك الشخصي .. فهو في أبسط صورة يقوم بتسجيل كل طريقة قمت بها على لوحة المفاتيح منذ أول لحظة للتشغيل ... وتشمل هذه كل بياناتك السرية أو حساباتك المالية أو محادثتك الخاصة على الانترنت أو رقم بطاقة الائتمان الخاصة بك أو حتى كلمات المرور التي تستخدمها لدخولك على الانترنت والتي قد يتم استخدامها بعد ذلك من قبل الجاسوس الذي قام بوضع البرنامج على حاسبك الشخصي

لماذا صممت البرامج التي تستخدم أحصنة طروادة ؟

تصميم هذه البرامج في البداية كان لأهداف نبيلة مثل معرفة ما يقوم به الأبناء أو الموظفون على جهاز الحاسب في غيابك من خلال ما يكتبونه على لوحة المفاتيح . ويوجد العديد من البرامج المنتشرة على الانترنت والتي تستطيع من خلالها التنصت وتسجيل وحفظ كل ما نكتبه على لوحة المفاتيح . من هذه البرامج برنامج يدعى Invisible KeyLloger، والذي يستطيع ان يحتفظ في ملف مخفي بكل ما قمت بكتابته على لوحة المفاتيح مصحوبة بالتاريخ والوقت الذي قمت فيه بعمليات الكتابة هذه ، حيث سيمكنك الإطلاع على الملف المسجل به كل ما تم كتابته على لوحة مفاتيح الحاسب (والتي لن يستطيع أحد معرفة مكانه

الا واضعه) والتأكد من عدم وجود جمل دخيلة أو محاولات اقتحام لم تقم أنت بكتابتها .. أو التأكد مما إذا كان أحد يقوم باستخدام حاسبك والإطلاع على بياناتك في غيابك والتأكد من عدم استخدامهم للانترنت في الولوج على شبكات غير أخلاقية أو التحدث بأسلوب غير لائق من خلال مواقع الدردشة على الانترنت، أيضا يزعم هؤلاء المصممين ان فوائد البرنامج الذي قاموا بتصميمه تظهر حينما تكتشف ان نظام الويندوز أو البرنامج الذي تستخدمه قد توقف فجأة عن العمل دون ان تكون قد قمت بحفظ التقرير الطويل الذي كنت تقوم بكتابته .. حيث ان التقرير بالكامل سيكون موجود منه نسخة إضافية بالملف المخفي ، أيضا من فوائد البرنامج مراقبة سير العمل والعاملين تحت إدارتك للتأكد من عدم قيامهم باستخدام الحاسب الشخصي لأغراض شخصية والتأكد من عدم إضاعتهم لوقت العمل واستغلاله بالكامل لتحقيق أهداف الشركة

خطورة برامج حصان طروادة

تعد برامج حصان طروادة واحدة من أخطر البرامج المستخدمة من قبل الهاكرز والدخلاء .. وسبب ذلك يرجع إلى انه يتيح للدخيل الحصول على كلمات المرور passwords والتي تسمح له ان يقوم بالهيمنة على الحاسب بالكامل .. كذلك تظهر هذه البرامج للدخيل الطريقة (المعلومات) التي يمكنه من خلالها الدخول على الجهاز بل والتوقيتات الملائمة التي يمكن خلالها الدخول على الجهاز... الخ، المشكلة أيضا تكمن في ان هذا الاقتحام المنتظر لن يتم معرفته أو ملاحظته حيث انه سيتم من خلال نفس الطرق المشروعة التي تقوم فيها بالولوج على برامجك وبياناتك فلقد تم تسجيل كل ما كتبته على لوحة المفاتيح في الملف الخاص بحصان طروادة .. معظم المستخدمين يعتقدون انه طالما لديهم برنامج مضاد للفيروسات فإنهم ليسوا معرضين للأخطار ، ولكن المشكلة تكمن في ان معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات . أما أهم العوامل التي تجعل حصان طروادة أخطر في بعض الأحيان من الفيروسات نفسها هي ان برامج حصان طروادة بطبيعتها خطر ساكن وصامت فهي لا تقوم بتقديم نفسها للضحية مثلما يقوم الفيروس الذي دائما ما يمكن ملاحظته من خلال الإزعاج أو الأضرار التي يقوم بها للمستخدم و بالتالي فإنها لا يمكن الشعور بها أثناء أدائها لمهمتها وبالتالي فان فرص اكتشافها والقبض عليها تكاد تكون معدومة

و يعتمد الاختراق على ما يسمى بالريموت (remote) أي السيطرة عن بعد ، ولكي تتم العملية لا بد من وجود شيئين مهمين الأول البرنامج المسيطر وهو العميل والآخر الخادم الذي يقوم بتسهيل العملية بعبارة أخرى للاتصال بين جهازين لا بد من توفر برنامج على كل من الجهازين لذلك يوجد نوعان من البرامج ، ففي جهاز الضحية يوجد برنامج الخادم (server) وفي الجهاز الأخر يوجد برنامج المستفيد أو ما يسمى (client) . وتندرج البرامج التي سبق ذكرها سواء كانت العميل أو الخادم تحت نوع من الملفات يسمى حصان طروادة ومن خلالهما يتم تبادل المعلومات حسب قوة البرنامج المستخدم
في التجسس. ، وتختلف برامج التجسس في المميزات وطريقة الاستخدام .. لكنهما جميعا تعتمد على نفس الفكرة التي ذكرناها وذلك بإرسال ما نسميه الملف اللاصق Patch file أو برنامج الخادم والذي

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

يرسلـه المتجسس إلى جهاز الضحية فيقوم الأخير بحسن نية بتشغيل هذا الملف ظنا منه بأنه برنامج مفيد لكنه غالبا ما يفاجأ بعدم عمل الملف بعد النقر عليه فيظن انه ملف معطوب.. فيبحث عن شيء آخر أو برنامج ثاني ويهمل الموضوع بينما في ذلك الوقت يكون المتجسس قد وضع قدمه الأولى داخل جهـاز الضحـيـة،، ويتم الاتصال بين الجهازين عبر منفذ اتصال لكل جهاز ، قد يعتقد البعض ان هذا المنفـذ مـادي باسـتطاعته ان يراه أو يلمسه مثل منفذ الطابعة أو المأوس ، ولكنه جزء من الذاكرة له عنوان معين يتعرف عليـه الجهاز بأنـه منطقة يتم إرسال واستقبال البيانات عليها ويمكن استخدام عـدد كبيـر مـن المنافـذ للاتصـال وعـددها يقـارب ٦٥٠٠٠ منفذ تقريبا ، يميز كل منفذ الآخر رقمه فمثلا المنفذ رقم ٨٠٨٠ يمكن إجراء اتصال عن طريقة ، وفي نفس اللحظة يتم استخدام المنفذ رقم ٨٠٠٠ لإجـــراء اتصـــــــال أخـــــــــر

وعند الإصابة ببرنـامج الخادم فانه يقوم في أغلب الأحـوال بما يلي :

١- الاتجاه إلى ملف تسجيل النظام (registry) حيـث ان النظـام فـي كـل مـرة تقـوم بتشـغيل الوينـدوز يقـوم بتشغيل البرامج المساعدة في ملف تسجيل النظام مثل برامج الفيروسات وغيرها.
٢- يقوم بفتح ملف اتصال داخل الجهاز المصاب تمكن برنامج العميل من النفوذ
٣- يقوم بعملية التجسس وذلك بتسجيل كل ما يحدث أو عمل أشياء أخرى على حسب ما يطلـب منـه هـذا يعني ان الجهاز إذا أصيب فانه يصبح مهيأ للاختراق، وبرنامج الخـادم ينتظـر طلـب اتصـال فـي أي لحظـة عـن طريق المنفذ الذي قام بفتحه ، ويأتي طلب الاتصال بأحد طريقين :

ا- من قبل شخص يتعمد اختراق الجهاز المصاب بعينة، وذلك لعلمه بوجود معلومات تهمه أو لإصابة ذلك الجهاز بالضرر لأي سبب كان
ب- من قبل شخص لا يتعمد اختراق هذا الجهاز بعينة، ولكنه يقوم بعمل مسح scanning على مجموعة مـن الأجهزة في نطاق معين من العناوين لمعرفة أيها الذي لديه منافذ مفتوحة وبالتالي فهو قابل للاختراق.

ما هو رقم الآي بي أدرس (IP(Internet protocol:

===============

تنتمي لعائلة TCP/IP وهو عبارة عن بروتوكول يسمى IP اختصار Internet Protocol
فلكي يتواجد شخص معين على شبكة الانترنت لابد ان تكون له هوية تمثله وهـذه الهويـه هـي الاي بـي و تكون من أربع أرقام وكل مستخدم على الشبكة له رقم لا يمكن لآخر ان يدخل به في نفس الوقت
مثل السيارة التي في الطريق كل سيارة لها الرقم الخاص بها و مستحيل يكون في سيارة لها نفس الـرقم و يتكون من أربع مقاطع كل مقطع يكون من ٠ -----> ٢٥٥
و العنونة على الشبكة تتم عن طريق تقسيم العناوين إلى أربعة نطاقات
(A) (B) (C) (D)

١- فالمستخدم العادي يستخدم أي بي من نطاق D و اقصد عنوان على شكل مثال "١٦٣,٢,٦,٤"
وذلك يعني ان الأربعة مقاطع محدده و ثابتة لا تتغير .

٢- اما الشركات تمتلك اي بي من نطاق C فهي تمتلك عنوان على هيئة ***،١٩٣,٢٥٥,٣
و مالك هذا العنوان يستطيع إعطاء إي قيمة تتراوح بين ٢٥٥ ---> ٠ اي انه يعطي ٢٥٥ رقم مثل : -
١٩٣,٢٥٥,٣,١
١٩٣,٢٥٥,٣,٢
١٩٣,٢٥٥,٣,٣
.
.
.
١٩٣,٢٥٥,٣,٢٥٥

٣- نطاق B ويكون على شكل ***.***١٩٣,٢٢٥
و يستطيع صاحبه إعطاء أرقام مثل : -
١٩٣,٢٢٥'١'١
١٩٣,٢٢٥'١'٢
١٩٣,٢٢٥'١'٣
.
.
.
١٩٣,٢٢٥'٢'١

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

١٩٣,٢٢٥'٢'٢
١٩٣,٢٢٥'٢'٣
.
.
.
١٩٣,٢٢٥'٢٥٥,٢٥٥

٤- النطاق A وهو على شكل : ***.***.***١٢٤
وهذا النطاق هو الأكثر اتساعا و تستخدمه منظمات دوليه أو هيئات تعمل لخدمة الانترنت على مستوى العالم .

كيف يصاب جهازك بملف الباتش أو التروجان أو حتى الفيروسات:

==

الطريقة الأولى:
ان يصلك ملف التجسس من خلال شخص عبر المحادثة أو (الشات) وهي ان يرسل أحد الهاكر لك صورة أو ملف يحتوي على الباتش أو التروجان ! ولابد ان تعلم أخي المسلم انه بإمكان الهاكر ان يغرز الباتش في صورة أو ملف فلا تستطيع معرفته إلا باستخدام برنامج كشف الباتش أو الفيروسات حيث تشاهد الصورة أو الملف بشكل طبيعي ولا تعلم انه يحتوي على باتش أو فيروس ربما يجعل جهازك عبارة عن شوارع يدخلها الهاكر والمتطفلون!

الطريقة الثانية:
ان يصلك الباتش من خلال رسالة عبر البريد الإلكتروني لا تعلم مصدر الرسالة ولا تعلم ماهية الشخص المرسل فتقوم بتنزيل الملف المرفق مع الرسالة ومن ثم فتحه وأنت لا تعلم انه سيجعل الجميع يدخلون إلى جهازك ويتطفلون عليك ..

الطريقة الثالثة:
إنزال برامج أو ملفات من مواقع مشبوهة مثل المواقع الجنسية أو المواقع التي تساعد على تعليم التجسس !

الطريقة الرابعة:
الدخول إلى مواقع مشبوهة مثل المواقع الجنسية حيث انه بمجرد دخولك إلى الموقع فانه يتم تنزيل الملف في جهازك بواسطة كوكيز لا تدري عنها شيئا !!
حيث يقوم أصحاب مثل هذه المواقع بتفخيخ الصفحات فعندما يرغب أحد الزوار في الدخول إلى هذه الصفحات تقوم صفحات الموقع بإصدار أمر بتنزيل ملف التجسس في جهازك !

كيف يختار الهاكر "المخترق" الجهاز الذي يود اختراقه:

======================

بشكل عام لا يستطيع الهاكر العادي من اختيار كمبيوتر بعينه لاختراقه إلا إذا كان يعرف رقم الآي بي أدرس الخاص به كما ذكرنا سابقاً فانه يقوم بإدخال رقم الآي بي أدرس الخاص بكمبيوتر الضحية في برنامج التجسس ومن ثم إصدار أمر الدخول إلى الجهاز المطلوب !!
وأغلب المخترقين يقومون باستخدام برنامج مثل (IP Scan) أو كاشف رقم الآي بي وهو برنامج يقوم الهاكر باستخدامه للحصول على أرقام الآي بي التي تتعلق بالأجهزة المضروبة التي تحتوي على ملف التجسس (الباتش) ! ، ثم يتم تشغيل البرنامج ثم يقوم المخترق بوضع أرقام آي بي افتراضيه .. أي انه يقوم بوضع رقمين مختلفين فيطلب من الجهاز البحث بينهما فمثلاً يختار هذين الرقمين:

٢١٢,٢٢٤,١٢٣,١٠

٢١٢,٢٢٤,١٢٣,١٠٠

لاحظ آخر رقمين وهما: ١٠ و ١٠٠
فيطلب منه البحث عن كمبيوتر يحوي منفذ (كمبيوتر مضروب) بين أجهزة الكمبيوتر الموجودة بين رقمي الآي بي أدرس التالي بين : ٢١٢,٢٢٤,١٢٣,١٠ و ٢١٢,٢٢٤,١٢٣,١٠٠

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

وهي الأجهزة التي طلب منه الهاكر البحث بينها !
بعدها يقوم البرنامج بإعطائه رقم الآي بي الخاص بأي كمبيوتر مضروب يقع ضمن النطاق الذي تم تحديده مثل :
٢١٢,٢٢٤,١٢٣,٥٠

٢١٢,٢٢٤,١٢٣,٩٨

٢١٢,٢٢٤,١٢٣,٣٣

٢١٢,٢٢٤,١٢٣,٤٧
فيخبره ان هذه هي أرقام الآي بي الخاصة بالأجهزة المضروبة التي تحوي منافذ أو ملفات تجسس فيستطيع الهاكر بعدها من أخذ رقم الآي بي ووضعه في برنامج التجسس ومن ثم الدخول إلى الأجهزة المضروبة !

فكر ة عامة على أشهر برامج الهاكرز الخاصة بالأجهزة:

==================================

والآن هيا بنا نتعرف على أشهر البرامج ولكن لن نستخدم أي منها نظرا لانها معروفة عند برامج الحماية معرفة تامة بمعني ان جميع ملفات الباتشات تمسك بسهولة تامة من برامج الحماية .... ولكن أردت ان أوضح عمل هذه البرامج و فيما كانت تستخدم قبل ان تكون معروفة من قبل برامج الحماية

NetBus
من أقدم البرامج في ساحة الاختراق بالسيرفرات وهو الأكثر شيوعا بين مستخدمي المايكروسوفت شات وهو برنامج به العديد من الإمكانيات التي تمكن الهاكر من التحكم بجهاز الضحية وتوجد نسخ مختلفة أكثر حداثة من النت باس وكل نسخة منها أكثر تطوراً من الأخرى ..

SUB 7
برنامج ممتاز وغني عن التعريف .. تستطيع التحكم وتنسيق السيرفر ليعمل كيفما تشاء سواء من تغيير شكل أو طريقة عمل وهو ممتاز في مجال الاختراق بالبرامج ..

Hackers Utility
برنامج مفيد ورهيب للهاكرز وخاصة المبتدئين والمحترفين حيث انه يمتلك أغلب وأفضل إمكانيات مختلف برامج الهاكرز ويمكن من خلاله كسر الكلمات السرية للملفات المضغوطة وفك تشفير الملفات السرية المشفرة وكذلك تحويل عناوين المواقع إلى أرقام آي بي والعكس كما به العديد من الإمكانيات والمميزات التي يبحث عنها الكثير من الهاكرز..

Back Orifice
برنامج غني عن التعريف لما لفيروسه من انتشار بين أجهزة مستخدمي الانترنت ولكن حتى تستطيع اختراق أحد الأجهزة لابد ان يكون جهازك ملوثاً بنفس الفيروس المستخدم ☹..

Deep Throat 2.0
يقوم هذا البرنامج بمسح الملف (سيستراي) ويقوم باستبداله بالسيرفر الخاص به وهذا البرنامج فيه ميزة وهي انك تستطيع التحكم في المواقع اللي يزورها الضحية وتقوم بتوجيهه لأي مكان ترغب وبإمكان المتحكم غلق وفتح الشاشة وكذلك استخدامه عن طريق برنامج الإف تي بي ..

porter
برنامج يعمل Scan على ارقام الـ IP و الـ Ports

pinger
برنامج يعمل (Ping) لمعرفة إذا كان الضحية أو الموقع متصلاً بالانترنت أم لا ...

Ultrascan
أسرع برنامج لعمل Scan على جهاز الضحية لمعرفة المنافذ المفتوحة التي يمكنك الدخول إليه منها...

Girl Friend
برنامج قام بعمله شخص يدعى بـ(الفاشل العام) ومهمته الرئيسية والخطيرة هي سرقة جميع كلمات السر الموجودة في جهازك بما فيها باسوورد الأيميل وكذلك إسم المستخدم والرمز السري الذي تستخدمه لدخول الانترنت ..

ما احتياجاتي لاختراق أي يهودي أو مُعادي للإسلام:

==============================

من خلال ما تحدثنا عنه سابقا نستنتج الآتي:

١: برنامج اختراق ..

٢: ضحية نرسل لها الباتش وتقوم بفتحه ..

٣: أي بي الضحية و يمكن معرفته عن طريق برامج الشات المختلفة مثل برنامج الآي سي كيو أو عن طريق البريد الالكتروني..

ما هو الفايرول (Firewall):

===============

هي برامج تستخدم للحماية على الشبكة وتكون بين الجهاز و الشبكة فتمنع حدوث اي اتصال خارجي الا بأذنك . و من اشهرها (Zone alarm , Norton Security ..)

ولكن من الأفضل ان لا تستخدم هذه البرامج حتى لا تشعر بالملل ناحيتها، وأنصحك ان تنزل برنامج حماية من الفيروسات فهو وحده يكفي لصد أي ملف باتش حتى لو استقبلته عن طريق الخطأ.

كيف تعرف إذا كان جهازك مخترقاً أم لا ☺ :

=====================

في البداية تستطيع ان تعرف إذا كان جهازك مخترقاً من خلال معرفة التغيرات التي يحدثها الهاكرز في نظام التشغيل مثل فتح وغلق الشاشة تلقائياً أو وجود ملفات جديدة لم يدخلها أحد أو مسح ملفات كانت موجودة أو فتح مواقع انترنت أو إعطاء أمر للطابعة بالإضافة إلى العديد من التغيرات التي تشاهدها وتعرفها وتعلم من خلالها عن وجود متطفل يستخدم جهازك ..

هذه الطريقة تستطيع من خلالها ان تعرف هل دخل أحد المتطفلين إلى جهازك أم ان جهازك سليم منهم ..
افتح قائمة (Start) و منها اختر أمر (Run).
اكتب التالي: system.ini
ستظهر لك صفحة فاذهب للسطر الخامس فيها فإذا وجدت ان السطر مكتوب هكذا:

user. exe=user. exe
فاعلم ان جهازك لم يتم اختراقه من قبل الهاكرز.

أما إذا وجدت السطر الخامس مكتوب هكذا :

user. exe=user. exe *** *** ***
فاعلم ان جهازك قد تم اختراقه من أحد الهاكرز.
هذه الطريقة تعمل على ويندوز ٩٨ – me غير ذلك فلا تعمل.

- كما توجد طريقة أخرى أيضا وتعمل على جميع أنظمة الويندوز وهي:

START>>RUN>>REGEDIT>>HKEY_LOCAL_MACHINE>>SOFTWARE>>
Microsoft>>WINDOWS>>CURRENTVERSION>>RUN

ستجد بها جميع البرامج التي تعمل مع تشغيل الويندوز وبالطبع فان أي برنامج باتش لا بد وان يعمل مع بداية الويندوز لذلك ستجد جميع البرامج التي تعمل مع بداية الويندوز في هذا المكان أما إذا أردت ان تعرف إذا كان جهازك مخترق أم لا فبالطبع يجب عليك ان تكون عارف أو حتى عندك خلفية بسيطة عن اسم الباتش حتى يتم حذفه أما إذا كنت لا تعرف فأنصحك بأول طريقة أفضل.

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

اختراق المواقع والبريد وبعض المصطلحات

هناك طرق عديدة لاختراق المواقع وهي :–

١: استخدام الثغرات..
٢: الدخول من بعض الأخطاء الموجودة في منتديات أو مجلات النيوك ..
٣: برامج اللست : و هي الأطول وللمبتدأين

وتعتمد برامج اللست عل لستة أو قائمة كبيرة تحتوي اكبر قدر ممكن من الكلمات بالاضافه إلى البرنامج الأساسي الذي يستخدم اللستة في تخمين كلمة السر .

١- استخدام الثغرات :
الثغرة الطريق لكي تكسب اعلى دخول للنظام ، من الممكن ان تكون من شخص غير مصرح إلى مشرك بسيط أو من مشترك بسيط إلى مدير النظام ، و هي تشتمل أيضا على تحطيم السرفرات ، و اغلب انواع الثغرات مكتوبة بلغة C ، وهي أقوى الطرق لاختراق المواقع و هي الاعقد و نستطيع ان نقول ان معظم الثغرات تستخدم للحصول على الروت و تكون أنت مدير نظام الجهاز الذي تريد اختراقه أو الموقع أو السرفر ...
و الثغرات تعتبر ملفات التي تسمح لك بالدخول عن طريق HTTP ، و تستطيع استخدام برامج السكان للحصول على ثغرات الموقع و هناك العديد من الثغرات و التي تتيح لك العديد من الاشياء مثل : -
١- قراءة ملفات .
٢- مسح و إضافة ملفات .
٣- روت .
و العديد ..
و الثغرة أصلا عبارة عن خطأ برمجي يستطيع منه المخترق التسلل إلى جهازك و كل ثغره عبارة عن كود معين (وليس عن برنامج كما يعتقد الكثير)، و يجب استخدام احد برامج السكان مثل (CGIscan أو Shadow..) لمعرفة ثغرات المواقع و من ثم الذهاب إلى موقع يقدم لك شرح و معلومات عن هذه الثغرة.

انواع الثغرات:

NT : Uni code , bofferoverfollow , fttp
UNIX : Get Access , CGI , buffer overfollow , PHP , send mail , Kernel exploits, rootkits, ProFTPD, WU-FTPD, X
Win 2000 : Uni code , bofferoverfollow , null session، في نظم ميكروسوفت
Liunx : Get Access , CGI , buffer overfollow , PHP , send mail , ProFTPD, WU-FTPD, Kernel Exploits, rootkits, X

ما هو Bufferoverflow
شبيها بهجمات الدوس و التي تحمل السيرفر حمولة ذائدة و تستخدم لإيقاف خدمة معينة مثل (ftp , pop , SMTP..) فمن الممكن الهجوم بها على سيرفر أف تي بي و سحب البسوردات منه ..

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

تدمير المواقع

وهي عن طريق برامج البنج وهي التي تبطئ الموقع و تثقله حتى يتوقف وتكون اما عن طريق الدوس أو برامج معينه مثل evil ping و برنامج الدرة ، كما انه مجرد الدخول إلى موقع و فتح أي صفحة بها صور يثقل عمل الموقع أو عمل بحث في الموقع ..

اختراق البريد

عدد لانهائي من الطرق و الحيل ولكنه صعب جدا جدا جدا

ومن أسهلها ان تخترق جهاز الضحية بالبيست أو الصب سفن وتذهب إلى قائمه الباسووردات المحفوظة (إذا كان حافظ الباسوورد سوف تجدها مع اسم بريده)

تدمير و تفجير البريد

وهو سهل و بسيط عن طريق إغراق البريد بإرسال حتى يتوقف و هناك برامج تسهل تلك العملية

==================================

Nuke Programs

وهي برامج تقوم بفصل صاحب الآي بي من الاتصال

==================================

Spoofing Programs

وهي تغير الآي بي إلى رقم آخر و يستفاد منها في الاختراق و بعد الأوقات تتوقف عليها ، كما انه يمكن ان نستخدمها في الحماية فعند الدخول الانترنت تعمل سبوف على الآي بي الخاص بك فلا يستطيع احد الوصول إلى جهازك غالبا ..

==================================

Cookies

هي عبارة عن ملفات يرسلها الموقع لمتصفحك و هي عبارة عن ملف مكتوب لا يستطيع أي موقع قراءته غير هذا الموقع و قد يكون به كلمات سر موقع أو اشتراك ...

وهي مزعجه في بعض الأحيان حيث أنها مثلا تسجل كل المواقع التي دخلتها و كل الصفحات التي شاهدتها و مدة مشاهدة كل صفحه ....

ويمكن مسح الكوكيز عن طريق الذهاب المجلد الخاص بها و حذف الملفات التي به C:\WINDOWS\Cookies و حذف الملفات التي توجد داخل هذا المجلد

==================================

Ports

وهي المنافذ التي يتسلل منها الهكرز لجهازك و من ثم التحكم فيه ..

==================================

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

Port Scanner

وهي برامج تفحص المنافذ المفتوحة لديك و تخبرك بها و تغلقها ..
مثل (Super Scan , Torjan Hunter)

=================================

ASM (كود الأسمبلي)

هو تمثيل رمزي للغة الأله لجهاز كمبيوتر محدد، يتم تحويل كود الأسمبلي إلى لغة الآله عن طريق مجمع .
البرمجة بلغة الأسمبلي بطيئة و تولد الكثير من الأخطاء و لكنها الطريقة الوحيدة لعرض كل أخر bit من الأداء من الهاردوير

=================================

الباك دوور

هو عبارة عن ثغرة في النظام الأمني متواجدة عمدا من قبل المصمم أو من قبل شخص أخر قام باحداث الثغرة عمدا . ليس من الشرط ان يكون الدافع لوجود كل ثغرة هو الأذية

=================================

Cipher

هو النص الذي تم تشفيره بواسطة نظام للتشفير .التشفير هو أي إجراء يستخدم في الكتابة السرية لتحويل النصوص العادية إلى نصوص مشفرة لمنع أي أحد من قراءة هذه البيانات إلى الشخص المقصود وصول البيانات إليه .

=================================

Compression

هو عمليه حسابيه لتقليل عدد البايت المطلوبة لتحديد كمية من البيانات عادة هو ترتيب البيكسل .

=================================

Cracker

هو الشخص الذي يحأول الحصول علي دخول غير مرخص لجهاز كمبيوتر هؤلاء الاشخاص غالبا خبثاء و لديهم العديد من الطرق للدخول إلى النظام.
لقد عرف هذا المصطلح عام ١٩٨٥ من قبل الهاكرز دفاعاً ضد استخدام الصحافة السيء لكلمة هاكر .

=================================

ECC = Error checking and correction

معناها فحص الأخطاء و تصحيحها وهي مجموعة من الطرق لتتبع الأخطاء في البيانات المرسلة أو المخزنة و تصحيحها .
يتم عمل هذا بعدة طرق و كلها تدخل بعض من أشكال التشفير أبسط أشكال تتبع الأخطاء هو اضافة بايت التعادل أو بالفحص الدوري المتزايد، ليس فقط بمقدور البايت المتعادل ان يقوم بتتبع الأخطاء التي حدثت بل يستطيع تحديد أي بايت تم عكسها و هل يجب إعادة عكسها استعادة البيانات الأصليه ، وكلما زاد عدد البايتس المضافة كلما زادت فرصة تعقب الأخطاء و تصحيحها

=================================

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

Encryption

هو أي اجراء يستعمل في الكتابة السرية لتحويل النصوص العادية إلى نصوص مشفرة و ذلك حتي لا يتمكن أي أحد من قراءة تلك البيانات ما عدا الشخص المقصود وصول البيانات إليه .
هناك العديد من أنواع تشفير البيانات و هذه الأنواع هي قواعد أمن الشبكة .

Kernel

هو الجزء الرئيسي في الويندوز إلى ونكس أو في أي نظام تشغيل و هو المسئول عن تخصيص المصادر و الأمن و خلافه .

الفيروسات

ما هو الفيروس:
========

هو برنامج مكتوب بإحدي لغات البرمجة يستطيع التحكم في برامج الجهاز و إتلافها و تعطيل عمل الجهاز كله و تستطيع نسخ نفسها ..

كيف تحدث الإصابة بالفيروسات:
=================

يتنقل الفيروس إلى جهازك عندما تقوم بنقل ملف ملوث بالفيروس إلى جهازك و ينشط الفيروس عند محأولة فتح ذلك الملف و قد يصل ذلك الفيروس من عدة أشياء لك منها انك قد نزلت ملف عليه فيروس من الانترنت أو قد وصلك على البريد على هيئة Attachment وو .... الخ ، كما ان الفيروس عبارة عن برنامج صغير و ليس من شرطا ان يكون للتخريب فمثلا هناك فيروس صممه أحد الفلسطينيين يفتح لك واجهه و يبين بعض الشهداء الفلسطنين و يعطيك بعض المواقع عن فلسطين ...
ويمكن عمل هذا الفيروس بطرق كثيره و بسيطة حيث انك يمكن تصميمه بلغات البرمجة أو حتى باستخدام Notpad

أضرار الفيروسات :-
=============

١- انشاء بعض الباد سيكتورس (Bad Sectors) والتي تتلف جزء من الهارد الخاص بك مما يمنعك من استخدام جزء منه ..
٢- إبطاء عمل الجهاز بصوره ملحوظة ..
٣- تدمير بعض الملفات ..
٤- تخريب عمل بعض البرامج و قد تكون هذه البرامج مثل الحماية من الفيروسات مما يشكل خطر رهيب ..
٥- اتلاف بعض اجزاء الجهاز (Bios) و الذي قد يجعلك تتضطر إلى تغير المزروت (Mother Board) و الكروت كلها ..
٦- قد تفاجأ بختفاء سيكتور من الهارد ..
٧- عدم التحكم في بعض اجزاء الجهاز ..
٨- انهيار نظام التشغيل ..
٩- توقف عمل الجهاز بصوره كاملة ..

خصائص الفيروسات:
==========

١- نسخ نفسه و الانتشار في الجهاز كله ..
٢- التغير في بعض البرامج المصابة مثل اضافة مقطع إلى ملفاتا لنوت باد في الاخر ..
٣- فك و تجميع نفسها و الاختفاء ..
٤- فتح منفذ ما في الجهاز أو تعطيل عمل بعض الاجزاء فيه ..
٥- يضع علامة مميزه على البرامج المصابة تسمى (Virus Mark)
٦- البرنامج المصاي بالفيروس يصيب البرامج الاخرى عن طريق وضع نسخه من الفيروس بها ..
٧- البرامج المصابة من الممكن ان تعمل عليها دون الشعور بأي خلل فيها لفتره ..

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

مما يتكون الفيروس:
===========

١- برنامج فرعي ليصيب البرامج التنفيذية ..
٢- برنامج فرعي لبدء عمل الفيروس ..
٣- برنامج فرعي لبدء التخريب ..

ماذا يحدث عند الاصابة بفيروس:
=================

١- عند فتح برنامج مصاب بالفيروس يبدء الفيروس بالتحكم في الجهاز و يبدء بالبحث عن ملفات ذات امداد exe. أو com. أو bat. .. حسب الفيروس و ينسخ نفسه بها..
٢- عمل علامة خاصة في البرنامج المصاب (Virus Marker) و تختلف من فيروس لاخر ..
٣- يقوم الفيروس بالحث عن البرامج و فحص إذا كانت بها العلامه الخاصة به ام لا و إذا كانت غير مصابه ينسخ نفسه بها ..
٤- إذا وجد علامته يكمل البحث في باقي البرامج و يصيب كل البرامج ..

ما هي مراحل العدوى :
============

١- مرحلة الكمون : حيث يختبأ الفيروس في الجهاز لفترة ..
٢- مرحلة الانتشار : و يبدء الفيورس في نسخ نفسه و الانتشار في البرامج و إصابتها و ووضع علامته فيها ..
٣- مرحلة جذب الزناد: و هي مرحلة الانفجار في تاريخ معين أو يوم .. مثل فيروس تشرنوبيل ..
٤- مرحلة الأضرار : و يتم فيها تخريب الجهاز ..

خطوات عمل الفيروس -:
===========

تختلف طريقة العدوى من فايروس لاخر و من نوع لاخر و هذا شرح مختصر لكيفية عمل الفيروسات : -
١- تحدث العدوى لبرنامج تنفيذي و لن تشعر باي تغيير فيه .
٢- عندما يبدأ البرنامج المصاب بالعمل يبدا نشاط الفيروس كما يلي : -
أ- ينفذ البرنامج الفعي الخاص بالبحث ، فيبحث الفيروس عن البرامج ذات الامتداد exe. أو com. أو .. و ان واجد اي منها يحضر جدزء صغير من بداية البرنامج إلى الذاكرة و من ثم يبحث عن علامته فان وجدها ترج البرنامج و بحث عن غيره و إذا لم يجدها يضعها في أول البرنامج .
ب- بعد ذلك تكون حدثت العدوى فتحدث عملة التخريب التي تسبب الاخطاء عند عمل البرنامج المصاب .
٣- بعد ذلك يعود التحكم للبرنامج مره اخرى (بعد ان كان الفيروس يتحكم فيه) ليبدو انه يعمل بصورة طبيعية .
٤- بعد ذلم تكون عملية العدوى انتهت يتم التخلص من الفيروس الموجود في الملف التنفيذي الأول حيث ان الفيروس قد انتشر في البرامج الاخرى .

انواع الفيروسات :
========

١: فيروسات قطاع التشغيل (Boot Sector Virus)
وهو الذي ينشط في منطقة نظام التشغيل وهو من اخطر انواع الفيروسات حيث انه يمنعك من تشغيل الجهاز

٢: فيروسات الماكرو (Macro Virus)
وهي من أكثر الفيروسات انتشارا حيث انها تضرب برامج الأوفيس و كما انها تكتب بالورد أو Notpad

٣: فيروسات الملفات (File Virus)
وهي تنتشر في الملفات وعند فتح أي ملف يزيد انتشارها ..

٤: الفيروسات المخفية (Stealth Virus)
وهي التي تحأول ان تختبئ من البرامج المضادة للفيروسات و لكن سهل الإمساك بها

٥: الفيروسات المتحولة (Polymorphic virus)
وهي الأصعب على برامج المقأومة حيث انه صعب الإمساك بها وتتغير من جهاز إلى آخر في أوامرها .. ولكن مكتوبة بمستوى غير تقني فيسهل إزالتها

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

٦: فيروسات متعددة الملفات (Multipartite Virus)
تصيب ملفات قطاع التشغيل و سريعة الانتشار ..

٧: فيروسات الدودة (Worm)
وهو عبارة عن برنامج ينسخ نفسه على الاجهزه و يأتي من خلال الشبكة و ينسخ نفسه بالجهاز عدة مرات حتى يبطئ الجهاز وهو مصمم لإبطاء الشبكات لا الأجهزة و بعض الناس تقول ان هذا النوع لايعتبر فيروس حيث انه مصمم للإبطاء لا لأزاله الملفات و تخريبها ..

٨: الباتشات (Trojans)
وهو أيضا عبارة عن برنامج صغير قد يكون مدمج مع ملف آخر للتخفي عندما ينزله شخص و يفتحه يصيب الـ Registry و يفتح عندك منافذ مما يجعل جهازك قابل للاختراق بسهوله و هو يعتبر من أذكى البرامج ، فمثلا عند عمل سكان هناك بعض التروجان يفك نفسه على هيئة ملفات غير محدده فيمر عليها السكان دون التعرف علية ، و من ثم يجمع نفسه مره ثانيه

برامج المقاومة

========

كيف تعمل ؟

هناك طريقتان في البحث عن الفيروسات
١: عندما يكون الفيروس معروف من قبل برامج المقاومة فتبحث عن التغير المعروف لها مسبقا الذي يسببه ذلك الفيروس
٢: عندما يكون الفيروس جديد فتبحث عن نشئ غير طبيعي في الجهاز حتى تجده و تعرف أي برنامج مسبب له
و توقفه

ودائما و غالبا تظهر نسخ عديدة من الفيروس و لها نفس التخريب مع فروق بسيطة

اشهر الفيروسات

اشهر الفيروسات على الإطلاق هو تشيرنوبل و مالسيا و فيروس الحب Love وقريبا في الأسواق العالمية فيرس " تهامي ☺"

١٥ نصيحة لكي تكون هاكر محترف

١- ايجادة استخدام نظام وندوز و معرفة كل شيء عنه ..
٢- محاولة معرفة كل المعومات عن نظام لينوكس حتى لو لم و لن تستعمله فهو اساس اختراق المواقع ..
٣- ايجادة استخدام لغات برمجية على الأقل (Java , C++ ,visual basic , PHP) .
٤- معرفة كيفية عمل نظام التشغيل و اكتشاف ثغراته و كيفية إغلاقها أو استخدمها ..
٥- معرفة كيف تحمي جهازك حماية شبة كاملة (حيث لا توجد حماية كاملة)..
٦- ايجادة اللغة الإنجليزية (English is the key for the big gate of hacking).
٧- لا تعتمد أبدا على أنا فلان سوف يعلمك شيء لأنك لن تحصل عليه كاملا أبدا و كل ما يأتي بسرعه يذهب بسرعة.
٨- *ليس معنى كونك هاكر انت تدمر جهاز .*
٩- ايجادة استخدام اشهر برامج البتشات (Sub 7 , Netbus ,Hack attack >>) حيث ان بعض الثغرات تسمح لك بتحميل ملفات على الضحية فيمكنك تحميل باتش و من ثم التسلل إلى جهاز الضحية .

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

١٠- معرفة كيفية استخدام ثغرات المتصفح و بعض الثغرات الأخرى الشهيرة مثل النت بيوس (Net Bios) ..

١١- إجادة استخدام التلنت .

١٢- متابعة آخر الثغرات التي تم اكتشافها .

١٣- حاول ان تطور بعض الأساليب الخاصة بك .

١٤- ان تظل تقرأ كل ما يقابلك من ملفات .

١٥- لا تعتمد على القراءة في المنتديات العربية .

كيف احمي نفسي

____

١: التأكد من نظافة الملفات قبل فتحها مثل exe لأنها ملفات تشغيليه وإذا ارسلك واحد شـي وهـو مـاهو برنـامج وامتداده exe معناه ممكن يكون فيروس أو ملف باتش
٢: عمل سكان كامل على الجهاز كل أسبوع على الأكثر
٣: التأكد من تحديث الانتي فايروس كل أسبوع على الأقل (شركة نورتون تطرح تحديث كل يوم أو يومين)
٤: وضح Anti-Virus جيد و انا انصح بوضع انتي فيرس الشمسية
٥: لا تظل مدة طويلة متصل بالشبكة بحيث لو ان واحد دخل عليك ما يظل يخرب فيك و عند خروجك و دخولك مره اخرى للشبكة يغير آخر رقم من الايبي.
٦: هذا الموقع يفحص جهازك و يخبرك بنقاط الضعف و الحلول http://www.antionline.com
٧: لا تخزن كلمات المرور أو كلمات سر على جهازك (مثل كلمة المرور لاشتراكك في الانترنت أو البريد الكتروني أو ...)
٨: لا تفتح اي ملفات تكون وصلة على بريدك الا بعد التأكد من نظافتها ..
٩: إذا لاحظت حدوث اي شيء غريب مثل خلل في اي برامج أو خروج و دخول السي دي افصل الاتصال بالانترنت فورا و تأكد من نظافة الجهاز.

مواقف مع الهاكرز وما تم معي

- أحد الهاكرز المحترفين من حسن حظ الهاكر و من سوء حظ الضحية انه كان في شبكة بداخلها أكثر من ١١ حاسب في إسرائيل تم تدمير أكثر من ٦ أجهزة من خلال عملية مسح الهارد ديسك باستخدام برنـامج Pro Rat ☺ وقد كان ينتقل التروجان من جهاز لآخر عن طريق تنزيل الضحية للباتش الذي كان يحتوى علـى صـورة خليعة ☺ لكي يشاهدها أصدقائه .... ياللهول .... عشان ما يتفرجش علـى صـور وحشـة تـاني. بجد بجـد الشخص الهاكر ده مية مية ☺.

- أحد الهاكرز دخل على الجهاز الشخصي لإحدى الفتيات وأخذ يشـاهد مـا يحتويـه مـن صـور وملفـات ولفـت انتباهه ان الكاميرا موصلة بالجهاز فأصدر أمر التصوير فأخذ يشاهدها وهي تستخدم الكمبيـوتر ثـم أرسـل لهـا رسالة يخبرها فيها انها جميلة جداً جداً ولكن (يا ريت لو تقلل من كمية الماكياج) !! ☺

- أحد الهاكرز دخل إلى جهاز فتاة يهودية و أخذ يحاورها حتى انه بعد ذلك اكتشف انها بنت مسئول كبير في اسرائيل ... وعندما عرف بذلك ظل لمدة شهراً لا يدخل الانترنت خوفا من القبض عليه ☺.
- أحد الهاكرز المحترفين اعتاد ان يدخل على مواقع البنوك عبر الانترنت ويتسلل بكل سلاسة إلـى الأرصـدة والحسابات فيأخذ دولار واحد من كل غني ويضع مجموع الدولارات في رصيد أقل الناس حساباً !!

- أحد الهاكرز يدخل إلى أجهزة الناس ويقوم بحذف الصور الخليعة والملفـات الجنسـية ويعتبـر نفسـه بهـذا (مجرد فاعل خير) وهو بهذا ينسى انه (حرامي ولص ومتسلل) !!
- اعتاد الهاكرز على محاولة اختراق المواقع الكبيرة مثل موقع الياهووو وموقع مايكروسوفت ولكـنهم دائمـاً مـا يفشلون في مراميهم هذه بسبب الجدران النارية التي تضعها هذه الشركات والإجراءات الضخمة التي تتبعها لمنع أي هاكرز من دخول النظام ومع هذا ينجح الهاكر في اختراق النظام ولكن خلال أقل مـن خمـس دقـائق يستطيع موظفوها من إعادة الأمور إلى مجراها!!

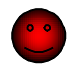
- يعد الاختراق والتجسس جريمة يحاسب عليها القـانون فـي الكثيـر مـن دول العـالم ولـذا لا تسـتغرب أخـي الكريم ان ترى الهاكر بجوار القاتل ومروج المخدرات واللصوص ولكن الفرق انه بمجرد خروج الهاكر من السجن يجد استقبالاً حافلاً من الشركات العالمية الكبرى التـي تسـارع إلـى توظيـف الهـاكرز بغـرض الاسـتفادة مـن

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com

خبرتهم في محاربة الهاكرز وكذلك للاستفادة من معلوماتهم في بناء برامج و أنظمة يعجز الهاكرز عن اقتحامها ..

- ***حكمة يؤمن بها كل الهاكرز*** : لا يوجد نظام تشغيل بدون منافذ ولا يوجد جهاز لا يحوي فجوة ولا يوجد جهاز لا يستطيع هاكر اقتحامه !!
- أغلب وأقوى الهاكر في العالم هم مبرمجو الكمبيوتر ومهندسو الاتصال والشبكات ولكن الأقوى منهم هم الشباب والمراهقون المتسلحون بالتحدي وروح المغامرة والذين يفرغون وقتهم لتعلم المزيد والمزيد في علم التجسس والتطفل على الناس، وعموماً مصير كل هؤلاء في الغالب **إلى السجن** ☹ **أو أكبر شركات الكمبيوتر والبرمجة في العالم** ☺ !!

- الآن تحولت الحروب من ساحات المعارك إلى ساحات الانترنت والكمبيوتر وأصبح الهاكرز من أقوى و أعتى الجنود الذين تستخدمهم الحكومات وخاصة (المخابرات) حيث يستطيعون التسلل بخفية إلى أجهزة وأنظمة العدو وسرقة معلومات لا تقدر بثمن وكذلك تدمير المواقع وغير ذلك .. وكذلك لا ننسى الحروب الجهادية الإلكترونية التي تدور رحاها بين العرب و اليهود والأمريكان والروس و... اللهم احفظنا !!



انتهى

تم الدرس الأول بالتمام و الكمال

إلى اللقاء في *الدرس الثاني* والذي يتحدث عن "فن الخداع و المراوغة" وشرح بعض برامج الهاكرز في طريقة الاختراق.

جمع وتأليف: ياسر رجب التهامي – ٢٠ سنة

طالب بالمعهد العالي للدراسات المتطورة بالهرم ٢٠٠٤ – ٢٠٠٨ مصر – جيزة

خاتمة

تم عمل فكرة هذا الكتاب بالشكل الآتي
قد أحضرت شخصا مبتدأ بعالم الحاسبات عموما وقد جعلته يسألني عن أي شيء خاص بالاختراق وكيف يتم وكيف يستخدم ... الخ وكنت أكتب كل سؤال يسألني إياه وعندما أذهب إلى البيت أبدأ باستنباط هذه الأسئلة وتنسيقها وأجاوب عليها إلى حد ما باللغة العربية وليس العامية المصرية لكي يستفيد بها جميع العرب إن شاء الله وبعد المراجعة عليها قد أتممت هذا الكتاب
و أخيراً.................،
أتمنى أن يوفقني الله لما يرضاه وان لا يستغل هذا الكتاب في إضرار الآخرين
يقول صلى الله عليه وسلم:
- **خيركم من تعلم العلم وعلمه.**
- **اطلبوا العلم ولو في الصين.**

و بذلك قد برّأت ذمتي وعدم كتماني لما أعلمه من أشياء الكثير لا يعلمها.
و أوعدكم إن شاء الله تعالى بأن أضيف الكثير والكثير من البرامج التعليمية إن شاء الله وكما وصلك هذا الكتاب فقد تصلك الكتب الأخرى ☺.

انتهى

-==*. -.*والسلام عليكم ورحمة الله وبركاته*.- .*==-

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com